#A36 INTEGERS 19 (2019)

THE UNIT STRUCTURE IN A QUOTIENT RING OF A QUADRATIC NUMBER FIELD

Brian D. Sittinger
Department of Mathematics, CSU Channel Islands, Camarillo, California

Marina C. Morales
ACE Charter High School, Camarillo, California

Received: 7/9/18, Accepted: 6/3/19, Published: 7/31/19

Abstract

The unit group structure of $\mathbb{Z}_m$ is well-known in number theory, largely due to the significance of primitive roots modulo m whenever they exist. We investigate the analogous problem for a quadratic number ring $\mathcal{O}$, determining the unit group structure of $\mathcal{O}/\mathfrak{a}$ for some fixed nonzero ideal $\mathfrak{a}$ in $\mathcal{O}$ along with a set of generators.

1. Introduction

It is often useful to represent a finite abelian group as a direct product of cyclic groups. With this description, it is easy to deduce many important properties of the group, such as its order, subgroup lattice, and rank. In this paper, we investigate the structure of the group of units in any quotient ring of a quadratic number field.

As a motivating example, we start with $\mathbb{Z}_m$, the ring of integers modulo m. This is a finite commutative ring whose units (elements having multiplicative inverses) form a multiplicative group which is denoted by $(\mathbb{Z}_m)^*$. It is a standard fact that a nonzero element $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x, m) = 1$. Moreover, the order of $(\mathbb{Z}_m)^*$ is given by the classic Euler phi function $\phi(m)$.

In order to find the group structure of $(\mathbb{Z}_m)^*$, recall that if $m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ is a prime factorization for m, then the Chinese Remainder Theorem induces the isomorphism

$$(\mathbb{Z}_m)^* \cong (\mathbb{Z}_{p_1^{n_1}})^* \times (\mathbb{Z}_{p_2^{n_2}})^* \times \cdots \times (\mathbb{Z}_{p_k^{n_k}})^*.$$

Thus, it suffices to understand $(\mathbb{Z}_{p^n})^*$ for any prime p. Its structure is given as follows [8]:

$$(\mathbb{Z}_{p^n})^* = \langle g \rangle \cong \mathbb{Z}_{p^n - p^{n-1}} \text{ for some } g \in \mathbb{Z}_{p^n} \text{ if } p \text{ is an odd prime,}$$

$$(\mathbb{Z}_{2^n})^* = \begin{cases} \{1\} & \text{if } n = 1, \\ \langle -1 \rangle \cong \mathbb{Z}_2 & \text{if } n = 2, \\ \langle -1 \rangle \times \langle 5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} & \text{if } n \geq 3. \end{cases}$$

If $(\mathbb{Z}_m)^*$ is cyclic, then any of its generators is called a *primitive root modulo m*. For example, when p is odd, g is a primitive root modulo p^n for any $n \in \mathbb{N}$. We can say more; by using this fact in conjunction with the Chinese Remainder Theorem, it is straightforward to deduce that a primitive root modulo m exists if and only if $m = 2, 4, p^n, 2p^n$ for any odd prime p and positive integer n.

We consider the more general problem of finding the unit group structure and a set of generators for a quotient ring of any quadratic number field over $\mathbb{Q}$. The inspiration for this problem came from Cross, who investigated this problem in the ring of Gaussian integers [3]. Subsequently, Buçaj investigated this problem in the ring of Eisenstein integers [2]. The results on the unit group structure for a quotient ring of any quadratic number field exist in the literature; in [5], Kohler recently compiled them together (so he could use these results to explicitly compute characters on these groups), proving these results via intricate counting arguments *without giving the generators*. We follow Cross' approach to find the generators in any such quotient ring. After reviewing the pertinent facts about quadratic number fields, we spend the remainder of this paper deriving the unit group structure for a quotient ring of any quadratic number field. From here, we answer the corresponding question concerning the existence of primitive roots in a quotient ring of a quadratic number field.

2. Background and Terminology

2.1. Quadratic Number Rings

In this section, we recall some basic concepts from algebraic number theory, as found in [6] and [8]. Let K denote an algebraic field over $\mathbb{Q}$ (that is, $[K : \mathbb{Q}] < \infty$) with $\mathcal{O}$ being its corresponding ring of integers. In this paper, we are primarily interested in the quadratic number field $\mathbb{Q}(\sqrt{d})$ for any square-free integer d. Its ring of integers $\mathcal{O}$, called a *quadratic number ring*, is the set $\{a + b\omega : a, b \in \mathbb{Z}\}$, where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \text{ mod } 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \text{ mod } 4. \end{cases}$$

Besides having the structure of a ring, $\mathbb{Q}(\sqrt{d})$ also has the operation of conjugation:

$$\overline{a + b\sqrt{d}} = a - b\sqrt{d} \text{ for any } a, b \in \mathbb{Q}.$$

With this operation, we define the norm of $\alpha \in \mathbb{Q}(\sqrt{d})$ by $N(\alpha) = \alpha\overline{\alpha}$. In particular, when $\alpha \in \mathcal{O}$, then $N(\alpha)$ is an integer.

Although we do not necessarily have unique factorization into irreducible elements in $\mathcal{O}$, we do have unique factorization into prime ideals in $\mathcal{O}$. We now give a description of the prime ideals in a quadratic number ring and how they arise from rational primes (primes in $\mathbb{Z}$).

Definition 1. Let p be a rational prime and $\mathcal{O}$ be a quadratic number ring.

(a) We say that p *splits* in $\mathcal{O}$ if $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ for distinct prime ideals $\mathfrak{p}, \overline{\mathfrak{p}}$ in $\mathcal{O}$.

(b) We say that p is *inert* in $\mathcal{O}$ if $\langle p\rangle$ is a prime ideal in $\mathcal{O}$.

(c) We say that p *ramifies* in $\mathcal{O}$ if $\langle p\rangle = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}$.

The resulting prime ideals are said to *lie above p*.

In the definition above, $\overline{\mathfrak{p}}$ is the ideal whose elements are conjugates to those in $\mathfrak{p}$. Next, we characterize the prime ideals in a quadratic number ring more precisely. A proof of this can be found in [6].

Theorem 1. *Let $\mathcal{O}$ be a quadratic number ring.*
For an odd rational prime p:

(a) p is inert in $\mathcal{O}$ if $(\frac{d}{p}) = -1$,

(b) p splits in $\mathcal{O}$ if $(\frac{d}{p}) = 1$,

(c) p ramifies in $\mathcal{O}$ if $p \mid d$.

For the rational prime 2:

(a) 2 is inert in $\mathcal{O}$ if $d \equiv 5 \bmod 8$,

(b) 2 splits in $\mathcal{O}$ if $d \equiv 1 \bmod 8$,

(c) 2 ramifies in $\mathcal{O}$ if d is even or $d \equiv 3 \bmod 4$.

It proves especially convenient to describe the generators of a prime ideal that lies above a rational prime p.

Lemma 1. *Suppose that $\mathfrak{p}$ lies above a ramifying prime p in a quadratic number ring $\mathcal{O}$.*
If p is odd, then $\mathfrak{p} = \langle p, \sqrt{d}\rangle$.

$$\textit{If } p = 2, \textit{ then } \mathfrak{p} = \begin{cases} \langle 2, \sqrt{d}\rangle \textit{ if } d \equiv 2 \bmod 4, \\ \langle 2, \sqrt{d} - 1\rangle \textit{ if } d \equiv 3 \bmod 4. \end{cases}$$

Proof. First, suppose that p is odd. Note that

$$\mathfrak{p}^2 = \langle p, \sqrt{d}\rangle^2 = \langle p^2, p\sqrt{d}, d\rangle.$$

Since $p \mid d$ but $p^2 \nmid d$, we know that $d = kp$ for some integer k not divisible by p. Thus $\gcd(k,p) = 1$, and there exist integers x and y such that $kx + py = 1$. Then, since $p^2, d \in \mathfrak{p}^2$, we have $dx + p^2y = p(kx+py) = p \in \mathfrak{p}^2$. Therefore, we conclude that $\langle p, \sqrt{d}\rangle^2 = \langle p \rangle$.

Next, assume that $p = 2$. If $d \equiv 2 \bmod 4$, then $\mathfrak{p} = \langle 2, \sqrt{d}\rangle$ by using the same arguments as we did when p was odd. If $d \equiv 3 \bmod 4$, then

$$\mathfrak{p}^2 = \langle 2, \sqrt{d}-1\rangle^2 = \langle 4, 2(\sqrt{d}-1), d+1-2\sqrt{d}\rangle.$$

Then, $2(\sqrt{d}-1) + (d+1-2\sqrt{d}) = d-1 \in \mathfrak{p}^2$. Finally, since $d-1 \equiv 2 \bmod 4$, we conclude that $2 \in \mathfrak{p}^2$, and the claim now immediately follows. □

In an effort to generalize the properties of $\mathbb{Z}$ to ideals in $\mathcal{O}$, we have a notion of *divides* in the context of ideals (which reduces to the usual definition of divisibility of an element in the case that all ideals are principal).

Definition 2. Given ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$, we say that $\mathfrak{a}$ *divides* $\mathfrak{b}$, written $\mathfrak{a} \mid \mathfrak{b}$, if $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$ for some ideal $\mathfrak{c}$ in $\mathcal{O}$.

In particular, any prime ideal in $\mathcal{O}$ divides the rational prime above which it lies. Moreover, it follows immediately from this definition that $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.

2.2. Quotient Rings of a Quadratic Number Field

Fix a nonzero ideal $\mathfrak{a}$ in a number ring $\mathcal{O}$, and consider the quotient ring $\mathcal{O}/\mathfrak{a}$. We first state a version of the Chinese Remainder Theorem for $\mathcal{O}$ (as any two distinct prime ideals are comaximal in $\mathcal{O}$; see [4] for a proof).

Theorem 2. *Let $\mathfrak{a} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\dots\mathfrak{p}_k^{n_k}$ be a prime factorization for the nonzero ideal $\mathfrak{a}$ in $\mathcal{O}$ where $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}$. Then,*

$$\mathcal{O}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{p}_1^{n_1} \times \mathcal{O}/\mathfrak{p}_2^{n_2} \times \cdots \times \mathcal{O}/\mathfrak{p}_k^{n_k}.$$

As we will be interested in the unit group $(\mathcal{O}/\mathfrak{a})^*$, the Chinese Remainder Theorem induces the isomorphism

$$(\mathcal{O}/\mathfrak{a})^* \cong (\mathcal{O}/\mathfrak{p}_1^{n_1})^* \times (\mathcal{O}/\mathfrak{p}_2^{n_2})^* \times \cdots \times (\mathcal{O}/\mathfrak{p}_k^{n_k})^*.$$

Hence, it suffices to study $(\mathcal{O}/\mathfrak{p}^n)^*$ for some fixed prime ideal $\mathfrak{p}$ in $\mathcal{O}$ and $n \in \mathbb{N}$.

As a first step in this endeavor, we first find a complete set of equivalence classes for $\mathcal{O}/\mathfrak{p}^n$. To assist us with this, we introduce the norm of an ideal.

Definition 3. The *norm* of a nonzero ideal $\mathfrak{a}$ in a number ring $\mathcal{O}$ is defined as $\mathfrak{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.

Note that the norm of an ideal is always finite and is related to the norm of an element $\alpha \in \mathcal{O}$ by $\mathfrak{N}(\langle\alpha\rangle) = N(\alpha)$. It can be shown that the norm of ideals is multiplicative: if $\mathfrak{a}, \mathfrak{b}$ are nonzero ideals in $\mathcal{O}$, then $\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$. Moreover, since a prime ideal $\mathfrak{p}$ is always maximal in $\mathcal{O}$, we know that $\mathcal{O}/\mathfrak{p}$ is a field. When $\mathcal{O}$ is a quadratic number ring, this implies that if $\mathfrak{p}$ is a prime ideal lying above the rational prime p, then $\mathfrak{N}(\mathfrak{p}) = p^2$ if p is inert, and $\mathfrak{N}(\mathfrak{p}) = p$ otherwise.

Theorem 3. *A complete set of congruence classes to a quadratic number ring $\mathcal{O}$ modulo a power of a prime ideal $\mathfrak{p}$ are given as follows:*

(a) If $\mathfrak{p}$ lies above a split prime p, then $\mathcal{O}/\mathfrak{p}^n = \{0, 1, \ldots, p^n - 1\}$.

(b) If p is inert, then $\mathcal{O}/\mathfrak{p}^n = \{a + b\omega\ :\ a, b = 0, 1, \ldots, p^n - 1\}$.

(c) If $\mathfrak{p}$ lies above a ramifying prime p, then for any $m \in \mathbb{N}$:
$\mathcal{O}/\mathfrak{p}^{2m} = \{a + b\omega\ :\ a, b = 0, 1, \ldots, p^m - 1\}$, and
$\mathcal{O}/\mathfrak{p}^{2m+1} = \{a + b\omega\ :\ a = 0, 1, \ldots, p^{m+1} - 1,\ \text{and}\ b = 0, 1, \ldots, p^m - 1\}$.

Proof. By the remarks preceding this theorem, along with $\mathfrak{N}(\mathfrak{p}^n) = \mathfrak{N}(\mathfrak{p})^n$, we have the correct number of congruence classes for $\mathcal{O}/\mathfrak{p}^n$. Hence, it suffices to establish that the given congruence classes of $\mathcal{O}/\mathfrak{p}^n$ are distinct.

(a) Suppose that $\mathfrak{p}$ lies above a splitting rational prime p. If $a = b$ in $\mathcal{O}/\mathfrak{p}^n$ with $a, b \in \{0, 1, \ldots, p^n - 1\}$, then $\mathfrak{p}^n \mid \langle a - b\rangle$. By conjugation, this yields $\overline{\mathfrak{p}}^n \mid \langle a - b\rangle$. Since $\gcd(\mathfrak{p}, \overline{\mathfrak{p}}) = \langle 1\rangle$, this implies that $\mathfrak{p}^n\overline{\mathfrak{p}}^n = \langle p^n\rangle \mid \langle a - b\rangle$, which is equivalent to $p^n \mid (a - b)$. Since $a, b \in \{0, 1, \ldots, p^n - 1\}$, we conclude that $a = b$.

(b) Next, suppose that p is inert so that $\mathfrak{p} = \langle p\rangle$. If $a + b\omega = c + d\omega$ in $\mathcal{O}/\mathfrak{p}^n$ for some $a, b, c, d \in \{0, 1, \ldots, p^n - 1\}$, then $(a - c) + (b - d)\omega = 0$ in $\mathcal{O}/\mathfrak{p}^n$. This implies that $p^n | (a - c)$ and $p^n | (b - d)$. Since a, b, c, d are between 0 and $p^n - 1$ inclusive, we conclude that $a = c$ and $b = d$.

(c) Finally, suppose that $\mathfrak{p}$ lies above a ramifying prime p. If $n = 2m$, then the distinctness of the given congruence classes is proved as in the inert case. Now, suppose $n = 2m + 1$ and $a + b\omega = c + d\omega$ in $\mathcal{O}/\mathfrak{p}^n$, where $a, c \in \{0, 1, \ldots, p^{m+1} - 1\}$ and $b, d \in \{0, 1, \ldots, p^m - 1\}$. Since $\mathfrak{p}^n = \langle p^m\rangle\mathfrak{p}$, it follows that $p^m \mid (b - d)$ and thus $b = d$. Therefore, $\mathfrak{p}^n = \langle p^m\rangle\mathfrak{p} \mid \langle a - c\rangle$, or equivalently $a - c = p^m \cdot k$ for some integer k, since the only rational elements in $\mathcal{O}$ are integers. Then, $\mathfrak{p} \mid \langle k\rangle$. Taking norms, we find that $p \mid k^2$ and thus $p \mid k$. Hence, $p^{m+1} \mid (a - c)$, and we conclude that $a = c$. □

As in $\mathbb{Z}$, the following notational shorthand will prove useful.

Definition 4. Fix a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}$. For any $\alpha, \beta \in \mathcal{O}$, we say that α *is congruent to β modulo* $\mathfrak{a}$, written $\alpha \equiv \beta \bmod \mathfrak{a}$, if $(\alpha - \beta) \in \mathfrak{a}$.

From this definition, we see that $\alpha \equiv \beta \bmod \mathfrak{a}$ if and only if α and β belong to the same coset in $\mathcal{O}/\mathfrak{a}$. It is straightforward to check that the fundamental properties of congruences over $\mathbb{Z}$ carry over to those in $\mathcal{O}$ unchanged.

Now we turn our attention to analyzing $(\mathcal{O}/\mathfrak{a})^*$. We first consider a generalization of Euler's phi function for number rings.

Definition 5. Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Define the *phi function* as $\phi(\mathfrak{a}) = |(\mathcal{O}/\mathfrak{a})^*|$.

Its basic properties are reminiscent of its classical counterpart (see [1]), and we now quote its most essential facts for our purposes. First of all, if $\mathfrak{a}, \mathfrak{b}$ are relatively prime ideals in $\mathcal{O}$, then $\phi(\mathfrak{a}\mathfrak{b}) = \phi(\mathfrak{a})\phi(\mathfrak{b})$. Moreover, when $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$ and $n \in \mathbb{N}$, we have

$$\phi(\mathfrak{p}^n) = \mathfrak{N}(\mathfrak{p})^n - \mathfrak{N}(\mathfrak{p})^{n-1}.$$

Although it is not crucial to the work that follows, we next give a complete set of congruence classes for $(\mathcal{O}/\mathfrak{p}^n)^*$ by suitably restricting the congruence classes from Theorem 3.

Theorem 4. *Let $\mathcal{O}$ be a quadratic number ring.*

(a) Suppose that $\mathfrak{p}$ lies above a split prime p. Then, $a \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $p \nmid a$.

(b) Suppose that p is inert. Then, $a + b\omega \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $p \nmid a$ or $p \nmid b$.

(c) Suppose that $\mathfrak{p}$ lies above a ramifying prime p.

(i) If either p is odd and $d \equiv 3 \bmod 4$, or $p = 2$ and $d \equiv 2 \bmod 4$, then $a + b\omega \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $p \nmid a$.

(ii) If p is odd and $d \equiv 1 \bmod 4$, then $a + b\omega \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $p \nmid (2a + b)$.

(iii) If $p = 2$ and $d \equiv 3 \bmod 4$, then $a+b\omega \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $2 \nmid (a+b)$.

Proof. Since $\mathcal{O}$ has unique factorization into prime ideals, $a \in \mathcal{O}/\mathfrak{p}^n$ is a unit if and only if $\mathfrak{p} \nmid \langle a \rangle$. With this observation, we now prove this theorem via contraposition.

(a) Suppose that p splits. By Theorem 3, any $a \in \mathcal{O}/\mathfrak{p}^n$ can be rewritten as an equivalence class from $\{0, 1, \ldots, p^n - 1\}$. Then, $a \in \mathcal{O}/\mathfrak{p}^n$ is a not a unit if and only if both $\mathfrak{p} \mid \langle a \rangle$ and $\overline{\mathfrak{p}} \mid \langle a \rangle$. Since $\gcd(\mathfrak{p}, \overline{\mathfrak{p}}) = \langle 1 \rangle$, and $\langle p \rangle = \mathfrak{p}\overline{\mathfrak{p}}$, this implies that $\langle p \rangle \mid \langle a \rangle$ and thus $p \mid a$.

(b) Now, suppose that p is inert. Then, $\mathfrak{p} = \langle p \rangle$, and $a + b\omega \in \mathcal{O}/\mathfrak{p}^n$ is not a unit if and only if $\langle p \rangle \mid \langle a + b\omega \rangle$. Hence, $p \mid (a + b\omega)$, and this is true if and only if both $p \mid a$ and $p \mid b$.

(c) Finally, suppose that p ramifies. Note that $a+b\omega \in \mathcal{O}/\mathfrak{p}^n$ is not a unit if and only if $\alpha \mid (a+b\omega)$ for some $\alpha \in \mathfrak{p}$. We have three cases to consider.

First, suppose that p is odd and $d \equiv 3 \bmod 4$, or $p=2$ and $d \equiv 2 \bmod 4$. Then, taking norms and noting that $p \mid N(\alpha)$, we obtain $p \mid (a^2-db^2)$. Finally, since $p \mid d$ due to p ramifying, we conclude that $p \mid a$.

Next, suppose that p is odd and $d \equiv 1 \bmod 4$ (as a reminder, this means that $\omega = \frac{1+\sqrt{d}}{2}$). Since $\mathfrak{p} = \langle p, \sqrt{d}\rangle$, we have that $\alpha = p(x+y\omega)+\sqrt{d}(z+t\omega)$ for some integers t,x,y,z. Without loss of generality, we may assume that $p \nmid (2z+t)$; otherwise we can also write $\sqrt{d}(z+t\omega)$ as a multiple of p. Since $\alpha \mid (a+b\omega)$, this implies that $N(\alpha) \mid (a+b\omega)\overline{\alpha}$. Then, because $p \mid N(\alpha)$ and $p \mid d$, it follows upon expanding $(a+b\omega)\overline{\alpha}$ in terms of $\sqrt{d}$ that $p \mid (-4az-2at-2bz-bt) = -(2z+t)(2a+b)$. Thus, $p \mid (2a+b)$ as required.

Finally, suppose that $p=2$ and $d \equiv 3 \bmod 4$. Since $\mathfrak{p} = \langle 2, \sqrt{d}-1\rangle$, we have that $\alpha = p(x+y\sqrt{d})+(\sqrt{d}-1)(z+w\sqrt{d})$ for some integers w,x,y,z. Without loss of generality, we may assume that $2 \nmid (z-w)$; otherwise we can also write $(\sqrt{d}-1)(z+w\sqrt{d})$ as a multiple of 2. Since $\alpha \mid (a+b\sqrt{d})$, this implies that $N(\alpha) \mid (a+b\sqrt{d})\overline{\alpha}$. Then, because $2 \mid N(\alpha)$ and d is odd, it follows upon expanding $(a+b\omega)\overline{\alpha}$ that $2 \mid (az+aw+bz+bw) = (w+z)(a+b)$. Thus $2 \mid (a+b)$ as required. □

As a consequence of Theorems 3 and 4, it immediately follows for a quadratic number ring $\mathcal{O}$ that $(\mathcal{O}/\mathfrak{p}^n)^*$ has $p^{2n}-p^{2n-2}$ elements when $\mathfrak{p}$ lies above an inert prime, and $p^n - p^{n-1}$ elements when $\mathfrak{p}$ lies above a split or ramified prime, in accordance with the generalized phi function.

The following proposition is a variant of Hensel's lifting lemma in $\mathbb{Z}$ that will prove useful in the work that follows. This allows us to *lift* a solution to a polynomial congruence from one power of a prime ideal to the next power.

Proposition 1. *Suppose that $f(x) \in \mathcal{O}[x]$ and $\mathfrak{p}$ is a prime ideal in a number ring $\mathcal{O}$. If $x=\alpha \in \mathcal{O}$ is a solution to $f(x) \equiv 0 \bmod \mathfrak{p}^{n-1}$ for some $n \geq 2$ and $f(\alpha) \in \gcd(\langle f'(\alpha)\rangle, \mathfrak{p}^n)$, then $f(x) \equiv 0 \bmod \mathfrak{p}^n$ has a solution in $\mathcal{O}$.*

Proof. We first establish the following claim: If $\alpha, \beta \in \mathcal{O}$, then

$$f(\alpha+\beta) = f(\alpha)+\beta f'(\alpha)+\beta^2\gamma \text{ for some } \gamma \in \mathcal{O}.$$

To show this, note that for any $k \in \mathbb{Z}_{\geq 0}$, the binomial theorem yields

$$(\alpha+\beta)^k = \alpha^k + k\alpha^{k-1}\beta + \beta^2\delta_k \text{ for some } \delta_k \in \mathcal{O}.$$

Writing $f(x) = \sum_{k=0}^{n} \rho_k x^k$ for some $\rho_k \in \mathcal{O}$ and $n \in \mathbb{N}$, we have

$$\begin{aligned}
f(\alpha+\beta) &= \sum_{k=0}^{n} \rho_k (\alpha+\beta)^k \\
&= \Big[\sum_{k=2}^{n} \rho_k (\alpha^k + k\alpha^{k-1}\beta + \beta^2 \delta_k) \Big] + \rho_1(\alpha+\beta) + \rho_0 \\
&= \sum_{k=0}^{n} \rho_k \alpha^k + \beta \cdot \sum_{k=1}^{n} k\rho_k \alpha^{k-1} + \beta^2 \cdot \sum_{k=0}^{n} \rho_k \delta_k \\
&= f(\alpha) + \beta f'(\alpha) + \beta^2 \gamma, \text{ where } \gamma = \sum_{k=0}^{n} \rho_k \delta_k.
\end{aligned}$$

Now, we are ready to prove this proposition. Suppose that $f(\alpha) \equiv 0 \bmod \mathfrak{p}^{n-1}$. We want to solve $f(x) \equiv 0 \bmod \mathfrak{p}^n$ by using α. To do this, we write $x = \alpha + \beta$ for some $\beta \in \mathfrak{p}^{n-1}$. Substituting this into $f(\alpha) \equiv 0 \bmod \mathfrak{p}^n$ and using the claim yields

$$f(\alpha+\beta) = f(\alpha) + \beta f'(\alpha) + \beta^2\gamma \equiv 0 \bmod \mathfrak{p}^n \text{ for some } \gamma \in \mathcal{O}.$$

Since $\beta^2 \in \mathfrak{p}^{2n-2}$ and $n \geq 2$, the previous relation reduces to

$$f(\alpha) + \beta f'(\alpha) \equiv 0 \bmod \mathfrak{p}^n.$$

This is solvable for β if and only if $f(\alpha) \in \gcd(\langle f'(\alpha) \rangle, \mathfrak{p}^n)$. □

In the next two sections, we explicitly give the unit group structure of any quotient ring $\mathcal{O}/\mathfrak{p}^n$, where $\mathfrak{p}$ is a prime ideal of a quadratic number ring $\mathcal{O}$.

3. Unit Group Structure for an Unramified Prime

3.1. Split Case

Theorem 5. *Suppose that $\mathfrak{p}$ lies above a split rational prime p. Then,*

$$(\mathcal{O}/\mathfrak{p}^n)^* \cong (\mathbb{Z}_{p^n})^*.$$

Proof. By Theorem 4, the set of congruence classes comprising $(\mathcal{O}/\mathfrak{p}^n)^*$ is formally the same as $(\mathbb{Z}_{p^n})^*$. This leads us to consider $\psi : (\mathcal{O}/\mathfrak{p}^n)^* \to (\mathbb{Z}_{p^n})^*$ defined by $\psi(a) = a$. Note that ψ is well-defined, because $\mathfrak{p} \mid \langle p \rangle)$. Moreover since ψ is a bijection by construction, we deduce that ψ is an isomorphism. In other words, $(\mathcal{O}/\mathfrak{p}^n)^* \cong (\mathbb{Z}_{p^n})^*$ as required. □

3.2. Inert Case

In this section, we assume that p is inert in $\mathcal{O}$. Before stating the group structure theorem, we give a couple lemmas to expedite the proofs of the group structure theorems (Theorems 6 and 7) that follow.

Lemma 2. *Let p be a rational prime and $k \in \mathbb{N}$.*
(a) If p is odd, then $(1+p\omega)^{p^k} = 1 + p^{k+1}\omega + p^{k+2}\gamma$ for some $\gamma \in \mathcal{O}$.
(b) $(1+2\omega)^{2^k} = 1 + 2^{k+1} + 2^{k+2}\gamma$ for some $\gamma \in \mathcal{O}$.

Proof. Let $\beta \in \mathcal{O}$ and r be a rational prime. Then by using a straightforward proof by induction on k in conjunction with the binomial theorem, we find that

$$(1+\beta r)^{r^k} = 1 + \beta r^{k+1} + \frac{1}{2}\beta^2(r^k - 1)r^{k+2} + \delta r^{k+2} \text{ for some } \delta \in \mathcal{O}.$$

With this identity, we can readily prove the lemma. Part (a) of the lemma follows directly from this claim by letting $r = p$ where p is an odd prime, $\beta = \omega$, and collecting like terms.

For part (b), observe that 2 is inert precisely when $d \equiv 5 \bmod 8$. Thus, $\omega = \frac{1+\sqrt{d}}{2}$, and $\omega^2 + \omega = \frac{d-1}{4} \equiv 1 \bmod 2$. Hence, letting $r = 2$ and $\beta = \omega$ yields

$$\begin{aligned}(1+2\omega)^{2^k} &= 1 + 2^{k+1}(\omega + (2^k - 1)\omega^2) + 2^{k+2}\delta \\ &= 1 + 2^{k+1} + 2^{k+2}\gamma \text{ for some } \gamma \in \mathcal{O}.\end{aligned}$$

□

Lemma 3. *Suppose that p is inert in $\mathcal{O}$. If $n \in \mathbb{N}_{>1}$, then the order of $1 + p\omega$ in $(\mathcal{O}/\mathfrak{p}^n)^*$ equals p^{n-1}.*

Proof. First, consider the case when p is odd. Letting $k = n-1$ in Lemma 2 yields

$$(1+p\omega)^{p^{n-1}} = 1 + p^n\omega + p^{n+1}\gamma \text{ for some } \gamma \in \mathcal{O}.$$

Therefore, $(1+p\omega)^{p^{n-1}} \equiv 1 \bmod p^n$, and thus the order of $1+p\omega$ divides p^{n-1}. Next, letting $k = n-2$ in Lemma 2 yields $(1+p\omega)^{p^{n-1}} \not\equiv 1 \bmod p^n$. Therefore, the order of $1+p\omega$ in $(\mathcal{O}/\mathfrak{p}^n)^*$ equals p^{n-1}.

Now, consider the case $p = 2$. Letting $k = n-1$ in Lemma 2 yields

$$(1+2\omega)^{2^{n-1}} = 1 + 2^n + 2^{n+1}\gamma \text{ for some } \gamma \in \mathcal{O}.$$

Hence, $(1+2\omega)^{2^{n-1}} \equiv 1 \bmod 2^n$, and the order of $1+2\omega$ divides 2^{n-1}. Next, letting $k = n-2$ in Lemma 2 and reducing modulo 2^n yields $(1+2\omega)^{2^{n-1}} \not\equiv 1 \bmod 2^n$. Therefore, the order of $1+2\omega$ in $(\mathcal{O}/\langle 2^n \rangle)^*$ equals 2^{n-1}. □

Now, we are able to give the group structure theorems for $(\mathcal{O}/\mathfrak{p}^n)^*$ in the case that p is inert. We start with the case when p is odd.

Theorem 6. *Let p be an inert odd prime and g be a primitive root modulo p^n. Then, there exists $\beta \in \mathcal{O}$ such that*

$$(\mathcal{O}/\mathfrak{p}^n)^* = \langle 1 + p\omega \rangle \times \langle g^{p-1} \rangle \times \langle \beta^{p^{n-1}} \rangle \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Proof. We have already examined $\langle 1 + p\omega \rangle$ in Lemma 3.

To construct g, the injective homomorphism $\psi : (\mathbb{Z}_{p^n})^* \to (\mathcal{O}/\mathfrak{p}^n)^*$ defined by $\psi(b) = b$ shows that we can view $(\mathbb{Z}_{p^n})^*$ as a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^*$. Since p is odd, $(\mathbb{Z}_{p^n})^*$ is cyclic of order $\phi(p^n) = p^{n-1}(p-1)$ with generator g. Consequently, $\langle g^{p-1} \rangle$ is isomorphic to a cyclic group of order p^{n-1}.

Finally, we construct β. Since p is prime in $\mathcal{O}$, and prime ideals in $\mathcal{O}$ are maximal, $\mathcal{O}/\mathfrak{p}$ is a field with $\mathfrak{N}(\mathfrak{p}) = p^2$ elements. Thus, $(\mathcal{O}/\mathfrak{p})^*$ is a cyclic group of order p^2-1; let β be a generator. Since $\beta^{p^2-1} \equiv 1 \bmod p$, we have $\beta^{p^2-1} = 1+\gamma p$ for some $\gamma \in \mathcal{O}$. Using the techniques of Lemma 2, $(\beta^{p^2-1})^{p^n-1} = (1 + \gamma p)^{p^{n-1}} = 1 + \delta p^n$ for some $\delta \in \mathcal{O}$. Therefore, $(\beta^{p^2-1})^{p^n-1} \equiv (\beta^{p^{n-1}})^{p^2-1} \equiv 1 \bmod p^n$. Letting t be the order of $\beta^{p^{n-1}}$, we have $t \mid (p^2 - 1)$. Then, $\beta^{tp^{n-1}} \equiv 1 \bmod p$ implies that $(p^2 - 1) \mid tp^{n-1}$, and thus $(p^2 - 1) \mid t$. Therefore, $t = p^2 - 1$ and $\langle \beta^{p^{n-1}} \rangle \cong \mathbb{Z}_{p^2-1}$.

Next, we show that these cyclic groups have pairwise trivial intersections. Since all elements of $\langle 1 + p\omega \rangle$ and $\langle g^{p-1} \rangle$ have orders that are powers of p, and $\langle \beta^{p^{n-1}} \rangle$ has order $p^2 - 1$, which is relatively prime to p, we can conclude that both $\langle 1 + p\omega \rangle$ and $\langle g^{p-1} \rangle$ have trivial intersections with $\langle \beta^{p^{n-1}} \rangle$.

It remains to show that $\langle 1 + p\omega \rangle$ and $\langle g^{p-1} \rangle$ have trivial intersection. Since both groups are cyclic with orders that are powers of the same prime p, $\langle 1+p\omega \rangle \cap \langle g^{p-1} \rangle$ is also cyclic of order p^k for some $k \in \{0, 1, \dots, n-1\}$. If $k \geq 1$, then $\langle 1+p\omega \rangle \cap \langle g^{p-1} \rangle$ contains a cyclic subgroup of order p. Since $1 + p\omega$ has order p^{n-1} in $(\mathcal{O}/\mathfrak{p}^n)^*$ by Lemma 2, it follows that $(1 + p\omega)^{p^{n-2}} = 1 + p^{n-1}\omega$ is an element in $\langle 1 + p\omega \rangle$ that has order p. Hence, all other elements of order p in $\langle 1 + p\omega \rangle$ have the form $(1 + p^{n-1}\omega)^k = 1 + p^{n-1}k\omega$, where $k \in \{1, 2, \dots, p-1\}$. Since none of these are in $\langle g^{p-1} \rangle$, we conclude that $k = 0$ and thus $\langle 1 + p\omega \rangle \cap \langle g^{p-1} \rangle = \{1\}$.

Hence, we can construct the direct product $\langle 1 + p\omega \rangle \times \langle g^{p-1} \rangle \times \langle \beta^{p^{n-1}} \rangle$, which is a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^*$ having order $p^{2n-2}(p^2 - 1)$. However, since the order of $(\mathcal{O}/\mathfrak{p}^n)^*$ is $\phi(\mathfrak{p}^n) = p^{2n-2}(p^2 - 1)$, the two groups are equal. □

To complete our discussion of the inert prime case, we now address the case when $p = 2$.

Theorem 7. *Suppose that 2 is an inert prime in a quadratic number ring $\mathcal{O}$.*

(a) $(\mathcal{O}/\langle 2 \rangle)^* = \langle \omega \rangle \cong \mathbb{Z}_3$.

(b) $(\mathcal{O}/\langle 2^2 \rangle)^* = \langle 1 + 2\omega \rangle \times \langle -1 \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *for some* $\alpha \in \mathcal{O}$.

(c) For each $n \geq 3$, *there exists* $\alpha \in \mathcal{O}$ *such that*

$$(\mathcal{O}/\langle 2^n \rangle)^* = \langle 1 + 2\omega \rangle \times \langle 1 + 4\omega \rangle \times \langle -1 \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Proof. (a) Since $\mathcal{O}/\langle 2\rangle$ is a field with 2^2 elements, $(\mathcal{O}/\langle 2\rangle)^*$ is a cyclic group of order $2^2-1=3$. Since $\omega \neq 1$ in $\mathcal{O}/\langle 2\rangle$, we conclude that ω is a generator for $(\mathcal{O}/\langle 2\rangle)^*$.

(b) Clearly -1 is an element of order 2 in $(\mathcal{O}/\langle 2^2\rangle)^*$. Moreover since $d \equiv 5 \bmod 8$, we have $(1+2\omega)^2 = 1+4\omega+4\omega^2 \equiv 1 \bmod 4$, as $\omega^2+\omega+\frac{1-d}{4}=0$. Thus, $1+2\omega$ has order 2 in $(\mathcal{O}/\langle 2^2\rangle)^*$.

Next, we construct an element α having order 3 in $(\mathcal{O}/\langle 2^2\rangle)^*$. To this end, recall that $\omega^3 \equiv 1 \bmod 2$. By Proposition 1, we can use this to find a solution $\alpha \in \mathcal{O}$ to $x^3 \equiv 1 \bmod 4$ (by taking $f(x)=x^3-1$ and noting that $f'(\omega)=3\omega^2 \notin \mathfrak{p}$).

Plainly, these three subgroups have pairwise trivial intersections, and the product of their orders equals $\phi(\langle 2^2\rangle) = 2^4-2^2 = 12$ as required.

(c) Since $1+2\omega$ has order 2^{n-1} from Lemma 2, we have $\langle 1+2\omega\rangle \cong \mathbb{Z}_{2^{n-1}}$. Since -1 has order 2, we take $\langle -1\rangle \cong \mathbb{Z}_2$. By Proposition 1, we can inductively find an element $\alpha \in \mathcal{O}$ such that $\alpha^3 \equiv 1 \bmod 2^n$. Hence, $\langle\alpha\rangle \cong \mathbb{Z}_3$.

For the fourth cyclic subgroup, we claim that $\langle 1+4\omega\rangle \cong \mathbb{Z}_{2^{n-2}}$. This follows from the fact that $(1+4\omega)^{2^{n-3}} \equiv 1+2^{n-1}\omega \mod 2^n$, which is easy to prove by induction in the style of the proof of Lemma 2.

We next observe that the four cyclic subgroups have pairwise trivial intersections. The only tricky case is showing that $\langle 1+4\omega\rangle \cap \langle 1+2\omega\rangle = \{1\}$. To this end, note that since $\langle 1+4\omega\rangle$ is cyclic of order 2^{n-2} and $\langle 1+2\omega\rangle$ is cyclic of order 2^{n-1}; if their intersection has a nontrivial element, then they both would share an element of order 2. This is impossible, since the elements of order 2 from the two cyclic subgroups are distinct, being $1+2^{n-1}\omega$ and $1+2^{n-1}$, respectively.

Finally, the product of the orders of the cyclic subgroups equals $\phi(\langle 2^n\rangle) = 2^{2n}-2^{2n-2} = 2^{2n-2}\cdot 3$ as required. □

4. Unit Group Structure for a Ramified Prime

Now, suppose that p ramifies in $\mathcal{O}$. We first give a result that is repeatedly used in subsequent subsections.

Lemma 4. *Suppose that p is a ramifying rational prime so that $\langle p\rangle = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}$. Then for any fixed $m \in \mathbb{N}$ and $r \in \{0,1\}$, there exists a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ isomorphic to $(\mathbb{Z}_{p^{m+r}})^*$.*

Proof. Fix $m \in \mathbb{N}$ and $r \in \{0,1\}$, and consider the map

$$\psi : (\mathbb{Z}_{p^{m+r}})^* \to (\mathcal{O}/\mathfrak{p}^{2m+r})^* \text{ defined by } \psi(a) = a.$$

Since $\mathfrak{p}^{2m+r} \mid \langle p\rangle^{m+r}$, it follows that ψ is a well-defined injective group homomorphism. Thus, $(\mathbb{Z}_{p^{m+r}})^*$ is isomorphic to a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$. □

4.1. Ramified Primes $p \geq 5$

As the cases for $p = 2$ and $p = 3$ ramifying are fairly involved, we first assume that $p \geq 5$ is a rational prime that ramifies in $\mathcal{O}$.

Theorem 8. *Suppose that $\mathfrak{p}$ lies above a ramifying prime $p \geq 5$.*

(a) $(\mathcal{O}/\mathfrak{p})^* = \langle g \rangle \cong \mathbb{Z}_{p-1}$, where g is a primitive root modulo p.

For any integer $m \geq 1$,

(b) $(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{m-1}}) \times \mathbb{Z}_{p^m}$, where g is a primitive root modulo p^m.

(c) $(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^m}) \times \mathbb{Z}_{p^m}$, where g is a primitive root modulo p^{m+1}.

Proof. (a) Note that $\mathcal{O}/\mathfrak{p}$ is a field with $\mathfrak{N}(\mathfrak{p}) = p$ elements. Hence, $(\mathcal{O}/\mathfrak{p})^*$ is a cyclic group with $p-1$ elements. Moreover, since $(\mathcal{O}/\mathfrak{p})^* = \{1, 2, \ldots, p-1\}$, we can generate this group by using a primitive root g modulo p.

(b, c) By Lemma 4, there exists a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ that is an isomorphic copy of $(\mathbb{Z}_{p^{m+r}})^*$. Since p is odd, $(\mathbb{Z}_{p^{m+r}})^*$ is cyclic of order $p^{m+r-1}(p-1)$ with generator g. (Note that $\langle g \rangle \cong \mathbb{Z}_{p^{m+r-1}(p-1)} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{m+r-1}}$.)

To show that $1 + \sqrt{d}$ has order p^m in $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ for both $r = 0$ and 1, we note that since $\sqrt{d} \in \mathfrak{p}$, the binomial theorem yields

$$(1 + \sqrt{d})^{p^k} = 1 + p^k\sqrt{d} + \gamma \text{ for some } \gamma \in \mathfrak{p}^{2k+2} \backslash \mathfrak{p}^{2k+3}.$$

By letting $k = m$, we see that $(1 + \sqrt{d})^{p^m} \equiv 1 \mod \mathfrak{p}^{2m+1}$ (and thus mod $\mathfrak{p}^{2m}$ as well), because $p \in \mathfrak{p}^2$ and $\sqrt{d} \in \mathfrak{p}$. However, letting $k = m-1$, we find that $(1 + \sqrt{d})^{p^{m-1}} \equiv 1 + p^{m-1}\sqrt{d} \not\equiv 1 \mod \mathfrak{p}^{2m}$ (and thus mod $\mathfrak{p}^{2m+1}$ as well), because $p^{m-1}\sqrt{d} \in \mathfrak{p}^{2m-1} \backslash \mathfrak{p}^{2m}$. Therefore, $1 + \sqrt{d}$ has order p^m in $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$.

Next, we show that $\langle 1 + \sqrt{d} \rangle$ and $\langle g \rangle$ have trivial intersection. Since both groups are cyclic whose orders are powers of the same prime p, $\langle 1 + \sqrt{d} \rangle \cap \langle g \rangle$ is also cyclic of order p^k for some $k \in \{0, 1, \ldots, m-1\}$. We want to show that $k = 0$. If $k \geq 1$, then $\langle 1 + \sqrt{d} \rangle \cap \langle g \rangle$ contains a cyclic subgroup of order p. Since $1 + \sqrt{d}$ has order p^m in $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ for both $r = 0$ and 1, it follows that $(1 + p\sqrt{d})^{p^{m-1}} = 1 + p^{m-1}\sqrt{d} + \gamma$ where $\gamma \in \mathfrak{p}^{2m} \backslash \mathfrak{p}^{2m+1}$. Hence, $(1 + p\sqrt{d})^{p^{m-1}} \in \langle 1 + \sqrt{d} \rangle$ that has order p, and thus all other elements of order p in $\langle 1 + \sqrt{d} \rangle$ are powers of this element. Since $(1 + p^{m-1}\sqrt{d} + \gamma)^k \equiv 1 + kp^{m-1}\sqrt{d} + k\gamma \mod \mathfrak{p}^{2m+1}$ for $k = 1, 2, \ldots, p-1$, none of these elements are in $\langle g \rangle$, and we conclude that $\langle 1 + \sqrt{d} \rangle \cap \langle g \rangle = \{1\}$.

Finally for both $r = 0$ and 1, since $\langle g \rangle \times \langle 1 + \sqrt{d} \rangle$ is a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ that has the same order as $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$, we are done. □

4.2. Ramified Prime 3

Now, suppose that 3 ramifies in $\mathcal{O}$ and $\mathfrak{p}$ lies above 3. First, we address the lower powers of $\mathfrak{p}$.

Theorem 9. *Suppose that $\mathfrak{p}$ lies above the ramifying prime 3.*

(a) $(\mathcal{O}/\mathfrak{p})^* = \langle -1\rangle \cong \mathbb{Z}_2$.

(b) $(\mathcal{O}/\mathfrak{p}^2)^* = \langle -1\rangle \times \langle 1+\sqrt{d}\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

(c) $(\mathcal{O}/\mathfrak{p}^3)^* = \langle 2\rangle \times \langle 1+\sqrt{d}\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_3) \times \mathbb{Z}_3$.

Proof. Since part (a) is trivial, we concentrate on the remaining parts.

(b) Clearly, -1 is an element of order 2. Next, we show that $1+\sqrt{d}$ has order 3 in $(\mathcal{O}/\mathfrak{p}^2)^*$. To do this, observe that $(1+\sqrt{d})^k \equiv 1 + k\sqrt{d} \bmod \mathfrak{p}^2$ by induction on k. From this claim, it follows that $(1+\sqrt{d})^3 \equiv 1 \bmod \mathfrak{p}^2$. However, since $\sqrt{d} \neq 0$ in $(\mathcal{O}/\mathfrak{p}^2)^*$, we conclude that the order of $1+\sqrt{d}$ is equal to 3 in $(\mathcal{O}/\mathfrak{p}^2)^*$.

Finally, the two cyclic groups from these generators have trivial intersection, because their orders are relatively prime. Since the order of $\langle g\rangle \times \langle 1+\sqrt{d}\rangle$ equals $\phi(\mathfrak{p}^2) = 3^2 - 3 = 6$, we are done.

(c) By Lemma 4, we can view $(\mathbb{Z}_{3^2})^*$ as a subgroup of $(\mathcal{O}/\mathfrak{p}^3)^*$. Note $(\mathbb{Z}_{3^2})^*$ is cyclic of order $3 \cdot 2 = 6$ with generator 2. As in part (b), we see that $1+\sqrt{d}$ has order 3 in $(\mathcal{O}/\mathfrak{p}^3)^*$. Finally, the cyclic subgroups have trivial intersection; otherwise, they would share a cyclic subgroup of order 3. However, since $(1+\sqrt{d})^k \equiv 1 + k\sqrt{d} \bmod \mathfrak{p}^2$ for both $k = 1, 2$ have nonzero $\sqrt{d}$ component modulo $\mathfrak{p}^2$, the claim immediately follows.

Since the order of $\langle g\rangle \times \langle 1+\sqrt{d}\rangle$ equals $\phi(\mathfrak{p}^3) = 3^2(3-1) = 18$, we are done. □

For higher powers of $\mathfrak{p}$, we must be more careful. First of all, note that since $3|d$ but $3^2 \nmid d$, $\frac{d}{3}$ is an integer congruent to 1 or 2 mod 3. It turns out that the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ depends on d in the aforementioned manner.

Theorem 10. *Suppose that $\mathfrak{p}$ lies above the ramifying prime 3. For any $m \geq 2$:*

(a) If $\frac{d}{3} \equiv 1 \bmod 3$, then

(i) $(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g\rangle \times \langle 1+\sqrt{d}\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^{m-1}}) \times \mathbb{Z}_{3^m}$,
where g is a primitive root modulo 3^m.

(ii) $(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g\rangle \times \langle 1+\sqrt{d}\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^m}) \times \mathbb{Z}_{3^m}$,
where g is a primitive root modulo 3^{m+1}.

(b) If $\frac{d}{3} \equiv 2 \bmod 3$, then for some $\alpha \in \mathcal{O}$:

(i) $(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g\rangle \times \langle 1+3\sqrt{d}\rangle \times \langle \alpha\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^{m-1}}) \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3$, *where g is a primitive root modulo 3^m.*

(ii) $(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g\rangle \times \langle 1+3\sqrt{d}\rangle \times \langle \alpha\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^{m}}) \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3$, *where g is a primitive root modulo 3^{m+1}.*

Proof. By Lemma 4, we can view $(\mathbb{Z}_{3^{m+r}})^*$ as a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$. Since 3 is odd, $(\mathbb{Z}_{3^{m+r}})^*$ is cyclic of order $2\cdot 3^{m+r-1}$ with generator g. In particular, note that $\langle g\rangle \cong \mathbb{Z}_{2\cdot 3^{m+r-1}} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^{m+r-1}}$.

Now, it remains to address the remaining cyclic subgroups.

(a) First of all, suppose that $\frac{d}{3} \equiv 1 \bmod 3$. We claim that $1+\sqrt{d}$ has order 3^m in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$.

For any positive integer k, the binomial theorem yields

$$(1+\sqrt{d})^{3^k} = 1 + \sum_{j=1}^{3^k} \binom{3^k}{j} (\sqrt{d})^j.$$

Letting $k=m$, we find that $(1+\sqrt{d})^{3^m} \equiv 1 \bmod \mathfrak{p}^{2m+1}$ since $\sqrt{d}\in\mathfrak{p}$ and $3^m \in \mathfrak{p}^{2m}$. Since this implies that $(1+\sqrt{d})^{3^m} \equiv 1 \bmod \mathfrak{p}^{2m}$, the order of $1+\sqrt{d}$ divides 3^m in $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ for both $r=0$ and 1.

Next, we let $k=m-1$ and rearrange terms to find that

$$(1+\sqrt{d})^{3^{m-1}} = \left(1+\binom{3^{m-1}}{2}d\right) + \left(3^{m-1}+\binom{3^{m-1}}{3}d\right)\sqrt{d} + \sum_{j=4}^{3^{m-1}} \binom{3^{m-1}}{j}(\sqrt{d})^j.$$

Now, we carefully analyze each term. First of all, since $\frac{d}{3}\equiv 1 \bmod 3$, we have $d = 3(1+3j)$ for some $j\in\mathbb{N}$. In particular, $d\in\mathfrak{p}^2\backslash\mathfrak{p}^3$. Moreover, since $\sqrt{d}\in\mathfrak{p}$ and $3\in\mathfrak{p}^2$, we have the following consequences: (i) $1+\binom{3^{m-1}}{2}d \in \mathfrak{p}^{2m}\backslash\mathfrak{p}^{2m+1}$; (ii) since $1+\frac{1}{2}(3^{m-1}-1)(3^{k-1}-2)(1+3j) \equiv 2 \bmod 3$, $\left(3^{m-1}+\binom{3^{m-1}}{3}d\right)\sqrt{d} \in \mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$; and (iii) $\sum_{j=4}^{3^{m-1}}\binom{3^{m-1}}{j}(\sqrt{d})^j \in \mathfrak{p}^{2m+2}$. Hence,

$$(1+\sqrt{d})^{3^{m-1}} \equiv 1+\alpha+\beta \bmod \mathfrak{p}^{2m+2}$$

for some nonzero $\alpha\in\mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$ and $\beta\in\mathfrak{p}^{2m}\backslash\mathfrak{p}^{2m+1}$.

Thus, $(1+\sqrt{d})^{3^{m-1}} \not\equiv 1 \bmod \mathfrak{p}^{2m}$ and therefore $(1+\sqrt{d})^{3^{m-1}} \not\equiv 1 \bmod \mathfrak{p}^{2m+1}$ as well. Hence, we can conclude that the order of $1+\sqrt{d}$ in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ equals 3^m.

(b) Now, suppose that $\frac{d}{3}\equiv 2 \bmod 3$.

First, we show that the order of $1+3\sqrt{d}$ equals 3^{m-1}. By the binomial theorem, $(1+3\sqrt{d})^{3^{m-1}} \equiv 1+3^m\sqrt{d} \bmod \mathfrak{p}^{2m+1}$. Moreover, since $\sqrt{d}\in\mathfrak{p}$ and $3\in\mathfrak{p}^2$, it follows that $(1+3\sqrt{d})^{3^{m-1}} \equiv 1 \bmod \mathfrak{p}^{2m+1}$, and the order of $1+3\sqrt{d}$ in $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ (and thus in $(\mathcal{O}/\mathfrak{p}^{2m})^*$) divides 3^{m-1} as well.

A similar calculation shows $(1+3\sqrt{d})^{3^{m-2}} \equiv 1+3^{m-1}\sqrt{d} \bmod \mathfrak{p}^{2m}$. However, $3^m\sqrt{d} \in \mathfrak{p}^{2m-1}$. Therefore, $(1+3\sqrt{d})^{3^{m-2}} \not\equiv 1 \bmod \mathfrak{p}^{2m}$ (and also mod $\mathfrak{p}^{2m+1}$). So, the order of $1+3\sqrt{d}$ in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ equals 3^{m-1}.

Note that $\langle 1+3\sqrt{d}\rangle \cap \langle g\rangle = \{1\}$, since any positive power of $1+3\sqrt{d}$ less than 3^{m-1} has a nonzero $\sqrt{d}$ coefficient.

For the other generator, given any integer $k \geq 4$, we need to find $\alpha \in \mathcal{O}\backslash\{1\}$ such that $\alpha^3 \equiv 1 \bmod \mathfrak{p}^k$. By direct calculation, we can take $\alpha = 1+\sqrt{d}$ for $k=4$. For $k>4$, we inductively invoke Proposition 1. Suppose we have found $\alpha \in \mathcal{O}\backslash\{1\}$ such that $\alpha^3 \equiv 1 \bmod \mathfrak{p}^k$. Letting $f(x) = x^3-1$, note that $f'(x) = 3x^2$. Although $f'(\alpha) \in \mathfrak{p}$, we have $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2\backslash\mathfrak{p}^3$ (since α is a unit in $\mathcal{O}/\mathfrak{p}^k$). Thus, indeed $f(\alpha) \in \gcd(f'(\alpha), \mathfrak{p}^k) = \mathfrak{p}^{k-2}$, and we can lift α to a solution to the congruence $x^3 \equiv 1 \bmod \mathfrak{p}^{k+1}$.

It remains to show $\langle\alpha\rangle \times (\langle 1+3\sqrt{d}\rangle \cap \langle g\rangle) = \{1\}$. Again, we prove this inductively on $k \geq 4$. This is true for $k=4$, since $1+\sqrt{d}$ and $(1+\sqrt{d})^2 \equiv 1+2\sqrt{d} \bmod \mathfrak{p}^4$ are not in $\langle 1+3\sqrt{d}\rangle \times \langle g\rangle$ (as their coefficients of $\sqrt{d}$ are not divisible by 3). Next, assume that there exist $x, y \in \mathbb{Z}$ such that $(x+y\sqrt{d})^3 \equiv 1 \bmod \mathfrak{p}^k$ with $3 \nmid y$. Then, $x+y\sqrt{d}$ lifts to a solution modulo $\mathfrak{p}^{k+1}$ of the form $(x+y\sqrt{d})+(r+s\sqrt{d})$ where $(r+s\sqrt{d}) \in \mathfrak{p}^k$. Then $3 \mid s$ and thus $3 \nmid (y+s)$, establishing the inductive step. □

4.3. Ramified Prime 2

Finally, we address the case where $\mathfrak{p}$ lies above the ramifying prime 2. Not so surprisingly, this is the most involved case. Recall that $\langle 2\rangle$ ramifies if and only if $d \equiv 2, 3 \bmod 4$. This gives some indication how the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ behaves. We first address the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ for small powers of $\mathfrak{p}$.

Theorem 11. *Suppose that $\mathfrak{p}$ lies above the ramifying prime 2.*

(a) $(\mathcal{O}/\mathfrak{p})^* = \{1\}$.

(b) $(\mathcal{O}/\mathfrak{p}^2)^* = \langle 1+\sqrt{d}\rangle \cong \mathbb{Z}_2$.

(c) $$(\mathcal{O}/\mathfrak{p}^3)^* = \begin{cases} \langle 1+\sqrt{d}\rangle \cong \mathbb{Z}_4 & \text{if } d \equiv 2 \bmod 4, \\ \langle \sqrt{d}\rangle \cong \mathbb{Z}_4 & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

(d) $$(\mathcal{O}/\mathfrak{p}^4)^* = \begin{cases} \langle 1+2\sqrt{d}\rangle \times \langle 1+\sqrt{d}\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \text{ if } d \equiv 2 \bmod 4, \\ \langle 1+2\sqrt{d}\rangle \times \langle \sqrt{d}\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \text{ if } d \equiv 3 \bmod 4. \end{cases}$$

(e) $$(\mathcal{O}/\mathfrak{p}^5)^* = \begin{cases} \langle -1\rangle \times \langle 1+2\sqrt{d}\rangle \times \langle 1+\sqrt{d}\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \text{ if } d \equiv 2 \bmod 4, \\ \langle -1\rangle \times \langle 1+2\sqrt{d}\rangle \times \langle \sqrt{d}\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \text{ if } d \equiv 3 \bmod 4. \end{cases}$$

Proof. (a) This follows from $\mathcal{O}/\mathfrak{p}$ being a field of order 2.

(b) By Theorem 4, $(\mathcal{O}/\mathfrak{p}^2)^*$ is a cyclic group with 2 elements. One such generator is $1+\sqrt{d}$, because $1+\sqrt{d} \neq 1$ and $(1+\sqrt{d})^2 \equiv 1+2\sqrt{d}+d^2 \equiv 1 \bmod \mathfrak{p}^2$. The last congruence follows from $2 \mid d$ and $\mathfrak{p}^2 = \langle 2 \rangle$.

(c) By Theorem 4, we know that $(\mathcal{O}/\mathfrak{p}^2)^*$ has order 4. In fact, it is cyclic.

If $d \equiv 3 \bmod 4$, observe that $(\sqrt{d})^4 \equiv 1 \bmod 4$ and thus $(\sqrt{d})^4 \equiv 1 \bmod \mathfrak{p}^3$, because $\mathfrak{p}^3 \mid \langle 4 \rangle$. Since $(\sqrt{d})^2 = d \not\equiv 1 \bmod \mathfrak{p}^3$, we conclude that $\sqrt{d}$ is a generator.

If $d \equiv 2 \bmod 4$, then although $(1+\sqrt{d})^2 = (1+d)+2\sqrt{d} \not\equiv 1 \bmod \mathfrak{p}^3$, we have $(1+\sqrt{d})^4 = 1+4\sqrt{d}+6d+4d\sqrt{d}+d^2 \equiv 1 \bmod 4$. Thus $(1+\sqrt{d})^4 \equiv 1 \bmod \mathfrak{p}^3$, and we conclude that $1+\sqrt{d}$ is a generator.

(d) Since $\mathfrak{p}^4 = \langle 4 \rangle$, it follows that $(1+2\sqrt{d})^2 \equiv 1 \bmod \mathfrak{p}^4$. Thus, $1+2\sqrt{d}$ has order 2 in $(\mathcal{O}/\mathfrak{p}^4)^*$. Next if $d \equiv 2 \bmod 4$, then $(1+\sqrt{d})^2 = (1+d)+2\sqrt{d} \not\equiv 1 \bmod \mathfrak{p}^4$, but $(1+\sqrt{d})^4 \equiv 1 \bmod \mathfrak{p}^4$; thus $1+\sqrt{d}$ has order 4 in $(\mathcal{O}/\mathfrak{p}^4)^*$. If $d \equiv 3 \bmod 4$, we have $(\sqrt{d})^2 = d \not\equiv 1 \bmod \mathfrak{p}^4$, but $(\sqrt{d})^4 \equiv 1 \bmod \mathfrak{p}^4$; thus $\sqrt{d}$ has order 4 in $(\mathcal{O}/\mathfrak{p}^4)^*$. For both cases of d, both $(\sqrt{d})^2$ and $(1+\sqrt{d})^2$ are not equal to $1+2\sqrt{d}$ in $(\mathcal{O}/\mathfrak{p}^4)^*$. This, combined with $\phi(\mathfrak{p}^4) = 8$, gives the desired group structure for $(\mathcal{O}/\mathfrak{p}^4)^*$.

(e) Plainly -1 is an element of order 2 for both $d \equiv 2, 3 \bmod 4$. Moreover, we claim that $1+2\sqrt{d}$ has order 2. When $d \equiv 2 \bmod 4$, $(1+2\sqrt{d})^2 = 1+4\sqrt{d}+4d \equiv 1 \bmod \mathfrak{p}^5$ (since $\sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$), and when $d \equiv 3 \bmod 4$, we note that $1-\sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$ to deduce that $(1+2\sqrt{d})^2 = 1+4\sqrt{d}(1-\sqrt{d}) \equiv 1 \bmod \mathfrak{p}^5$.

Next, we find a generator having order 4. When $d \equiv 2 \bmod 4$, we claim that $1+\sqrt{d}$ has order 4. To this end, $(1+\sqrt{d})^2 = (1+d)+2\sqrt{d} \not\equiv 1 \bmod \mathfrak{p}^5$, but since $8 \mid (6d+d^2)$ $(1+\sqrt{d})^4 \equiv 1+(6d+d^2)+4\sqrt{d}(1+d) \equiv 1 \bmod \mathfrak{p}^5$. When $d \equiv 3 \bmod 4$, we use $\sqrt{d}$, because $(\sqrt{d})^2 = d \not\equiv 1 \bmod \mathfrak{p}^5$, but $(\sqrt{d})^4 \equiv 1 \bmod \mathfrak{p}^5$. In both cases, the cyclic subgroups generated by this element of order 4 have trivial intersections with those generated by -1 and $1+2\sqrt{d}$.

Finally, since the order of the direct product of these three cyclic groups equals $\phi(\mathfrak{p}^5) = 16$ for both cases of d, we have the desired group structure for $(\mathcal{O}/\mathfrak{p}^5)^*$. □

Now, we consider higher powers of $\mathfrak{p}$. However, when $d \equiv 3 \bmod 4$, it turns out that we have to investigate $d \equiv 3$ and $7 \bmod 8$ separately.

Theorem 12. *Suppose that $\mathfrak{p}$ lies above the ramifying prime 2, and let $m \geq 3$.*

(a) If $d \equiv 2 \bmod 4$, then

$$(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle -1 \rangle \times \langle 5 \rangle \times \langle 1+\sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^m},$$
$$(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle -1 \rangle \times \langle 5 \rangle \times \langle 1+\sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^m}.$$

(b) If $d \equiv 7 \bmod 8$, then for some $\alpha \in \mathcal{O}$

$$(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle\alpha\rangle \times \langle 5\rangle \times \langle 1+2\sqrt{d}\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^{m-1}},$$
$$(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle\alpha\rangle \times \langle 5\rangle \times \langle 1+2\sqrt{d}\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}}.$$

(c) If $d \equiv 3 \bmod 8$*, then for some* $\alpha \in \mathcal{O}$

$$(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle -1\rangle \times \langle 1+2\sqrt{d}\rangle \times \langle\alpha\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}},$$
$$(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle -1\rangle \times \langle 1+2\sqrt{d}\rangle \times \langle\alpha\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m}}.$$

Proof. (a) Suppose that $d \equiv 2 \bmod 4$. By Lemma 4, we can view $(\mathbb{Z}_{2^{m+r}})^*$ as a subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$. Since $(\mathbb{Z}_{2^{m+r}})^* = \langle -1\rangle \times \langle 5\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m+r-2}}$, we have our generators for $\mathbb{Z}_2 \times \mathbb{Z}_{2^{m+r-2}}$.

It remains to find an element of order 2^m for both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$. We claim that one such element is $1+\sqrt{d}$. We prove this by induction on $m \geq 3$ by showing that

$$\text{(i) } (1+\sqrt{d})^{2^m} \equiv 1 \bmod \mathfrak{p}^{2m+1}, \text{ and (ii) } (1+\sqrt{d})^{2^{m-1}} \equiv 1+\gamma \not\equiv 1 \bmod \mathfrak{p}^{2m}$$

for some $\gamma \in \mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$. Note these readily imply that $(1+\sqrt{d})^{2^m} \equiv 1 \bmod \mathfrak{p}^{2m}$, and $(1+\sqrt{d})^{2^{m-1}} \not\equiv 1 \bmod \mathfrak{p}^{2m+1}$ as well.

For $m=3$, since $\sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$,

$$\begin{aligned}(1+\sqrt{d})^{2^3} &\equiv 1 + 8\sqrt{d} + 28(\sqrt{d})^2 + 56(\sqrt{d})^3 + 70(\sqrt{d})^4 + 0\\ &\equiv 1 + 28(\sqrt{d})^2 + 70(\sqrt{d})^4\\ &\equiv 1 + 7\cdot 2(\sqrt{d})^2(2+5d)\\ &\equiv 1 + 7\cdot 2^3(\sqrt{d})^2(3+5k) \text{ since } d = 2+4k \text{ for some integer } k\\ &\equiv 1 \bmod \mathfrak{p}^7.\end{aligned}$$

This establishes (i). For (ii), working modulo $\mathfrak{p}^6$ yields

$$\begin{aligned}(1+\sqrt{d})^{2^2} &\equiv 1 + 4\sqrt{d} + 6(\sqrt{d})^2 + 4(\sqrt{d})^3 + (\sqrt{d})^4\\ &\equiv 1 + 4\sqrt{d} + 6(\sqrt{d})^2 + (\sqrt{d})^4\\ &\equiv 1 + 4\sqrt{d} \text{ since } d \equiv 2 \bmod 4\\ &\not\equiv 1 \bmod \mathfrak{p}^6.\end{aligned}$$

Moreover, $4\sqrt{d} \in \mathfrak{p}^5\backslash\mathfrak{p}^6$, thereby finishing the inductive step.

Now we assume the claim is true for m and show it is true for $m+1$. To show (i), note that the inductive hypothesis yields $(1+\sqrt{d})^{2^m} = 1+\alpha$ for some $\alpha \in \mathfrak{p}^{2m+1}$. Then, $(1+\sqrt{d})^{2^{m+1}} = (1+\alpha)^2 = 1+2\alpha+\alpha^2$. Reducing modulo $\mathfrak{p}^{2m+3}$ immediately yields $(1+\sqrt{d})^{2^{m+1}} \equiv 1 \bmod \mathfrak{p}^{2m+3}$.

To establish (ii), by the inductive hypothesis, $(1+\sqrt{d})^{2^{m-1}} \equiv 1+\gamma \bmod \mathfrak{p}^{2m}$ for some $\gamma \in \mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$. So, we have $(1+\sqrt{d})^{2^{m-1}} = 1+\gamma+\delta$ for some $\delta \in \mathfrak{p}^{2m}$.

Then $(1+\sqrt{d})^{2^m} = (1+\gamma+\delta)^2 \equiv 1+2\gamma \not\equiv 1 \bmod \mathfrak{p}^{2m+2}$ as required, because $2\gamma \in \mathfrak{p}^{2m+1}\backslash\mathfrak{p}^{2m+2}$. This concludes the induction.

Since no nontrivial power of $1+\sqrt{d}$ is an integer, $\langle 1+\sqrt{d}\rangle \cap (\langle -1\rangle \times \langle 5\rangle) = \{1\}$. Finally, since the order of $\langle -1\rangle \times \langle 5\rangle \times \langle 1+\sqrt{d}\rangle$ equals $\mathfrak{N}(\mathfrak{p}^n)$ when $n \geq 6$, we have the desired unit group structure result.

(b) Now, suppose that $d \equiv 7 \bmod 8$.

We know that 5 has order 2^{m-2}, being one of the generators of $(\mathbb{Z}_{2^m})^*$.

It remains to find an element of order 2^{m-1} in $(\mathcal{O}/\mathfrak{p}^{2m+r})^*$ for both $r = 0, 1$. We claim that one such element is $1+2\sqrt{d}$. We prove this by induction on $m \geq 3$ by showing that

$$\text{(i) } (1+2\sqrt{d})^{2^{m-1}} \equiv 1 \bmod \mathfrak{p}^{2m+1}, \text{ and (ii) } (1+\sqrt{d})^{2^{m-2}} \equiv 1+\gamma \not\equiv 1 \bmod \mathfrak{p}^{2m}$$

for some $\gamma \in \mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$.

For $m = 3$, since $(\sqrt{d}-1) \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$, we have

$$\begin{aligned}(1+\sqrt{d})^{2^{3-1}} &\equiv 1+4(2\sqrt{d})+6(2\sqrt{d})^2+4(2\sqrt{d})^3+(2\sqrt{d})^4\\ &\equiv 1+16d+8(\sqrt{d}-1)\\ &\equiv 1 \bmod \mathfrak{p}^7.\end{aligned}$$

This establishes (i). For (ii), working modulo $\mathfrak{p}^6 = \langle 8\rangle$ yields

$$\begin{aligned}(1+\sqrt{d})^{2^{3-2}} &\equiv 1+2(2\sqrt{d})+(2\sqrt{d})^2\\ &\equiv 1+4\sqrt{d}(\sqrt{d}-1)\\ &\not\equiv 1 \bmod \mathfrak{p}^6.\end{aligned}$$

The last line follows from $4\sqrt{d}(\sqrt{d}-1) \in \mathfrak{p}^5\backslash\mathfrak{p}^6$, thereby finishing the inductive step.

Now we assume the claim is true for m and show it is true for $m+1$.
To show (i), by the inductive hypothesis, $(1+2\sqrt{d})^{2^{m-1}} \equiv 1 \bmod \mathfrak{p}^{2m+1}$. Thus, we can write $(1+2\sqrt{d})^{2^{m-1}} = 1+\alpha$ for some $\alpha \in \mathfrak{p}^{2m+1}$. Then, $(1+2\sqrt{d})^{2^m} = (1+\alpha)^2 = 1+2\alpha+\alpha^2$. Reducing modulo $\mathfrak{p}^{2m+3}$ yields $(1+2\sqrt{d})^{2^m} \equiv 1 \bmod \mathfrak{p}^{2m+3}$.

To establish (ii), we have $(1+2\sqrt{d})^{2^{m-2}} \equiv 1+\gamma \bmod \mathfrak{p}^{2m}$ for some $\gamma \in \mathfrak{p}^{2m-1}\backslash\mathfrak{p}^{2m}$ by the inductive hypothesis. Then, $(1+2\sqrt{d})^{2^{m-1}} = 1+\gamma+\delta$ for some $\delta \in \mathfrak{p}^{2m}$. Therefore, $(1+2\sqrt{d})^{2^m} = (1+\gamma+\delta)^2 \equiv 1+2\gamma \not\equiv 1 \bmod \mathfrak{p}^{2m+2}$ as required, because $2\gamma \in \mathfrak{p}^{2m+1}\backslash\mathfrak{p}^{2m+2}$. This concludes the induction.

For the third generator, we find an element of order 4. To make sure the cyclic subgroup generated by this element has trivial intersection with those generated by 5 and $1+2\sqrt{d}$, we make sure that its square equals -1. Hence, it suffices to solve $\alpha^2 \equiv -1 \bmod \mathfrak{p}^k$ for $k \geq 6$. We begin with $k = 4$, because we can let $\alpha = \sqrt{d}$. For $k > 4$, we inductively invoke Hensel lifting. Suppose we have found $\alpha \in \mathcal{O}$ such that $\alpha^2 \equiv -1 \bmod \mathfrak{p}^k$. Letting $f(x) = x^2 - 1$, then $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2 \backslash \mathfrak{p}^3$ (since α is a unit in $\mathcal{O}/\mathfrak{p}^k$). Thus, indeed $f(\alpha) \in \gcd(\langle f'(\alpha)\rangle, \mathfrak{p}^k) = \mathfrak{p}^{k-2}$ and we can lift α to a solution to $x^2 \equiv -1 \bmod \mathfrak{p}^{k+1}$.

Now, it is routine to show that the order of $\langle\alpha\rangle \times \langle 5\rangle \times \langle 1 + 2\sqrt{d}\rangle$ equals $\phi(\mathfrak{p}^n)$ for $n \geq 6$.

(c) Suppose that $d \equiv 3 \bmod 8$.

Clearly, -1 has order 2 and it can be checked using the binomial theorem that $1 + 2\sqrt{d}$ has order 2^{m-1}.

It remains to find a generator for $\mathbb{Z}_{2^{m-1}}$ and $\mathbb{Z}_{2^m}$, depending on m being even or odd, respectively. Since -5 has order 2^{m-2} and 2^{m-1} (as m is even or odd) respectively, we can construct a generator α that satisfies $\alpha^2 \equiv -5 \bmod \mathfrak{p}^n$ when $n \geq 6$. (Note that this cyclic subgroup generated by α necessarily has trivial intersection with those generated by -1 and $1 + 2\sqrt{d}$.)

Hence, it suffices to solve $\alpha^2 \equiv -1 \bmod \mathfrak{p}^k$ for $k \geq 6$. We begin with $k = 6$, because letting $\alpha = 4 + \sqrt{d}$ yields $(4 + \sqrt{d})^2 = 16 + 8\sqrt{d} + d \equiv -5 \bmod 8$. For $k > 6$, we inductively invoke Hensel lifting. Suppose we have found $\alpha \in \mathcal{O}$ such that $\alpha^2 \equiv -5 \bmod \mathfrak{p}^k$. Letting $f(x) = x^2 - 1$, we see that $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2 \backslash \mathfrak{p}^3$ (since α is a unit in $\mathcal{O}/\mathfrak{p}^k$). Thus, $f(\alpha) \in \gcd(\langle f'(\alpha)\rangle, \mathfrak{p}^k) = \mathfrak{p}^{k-2}$ and we can lift α to a solution to $x^2 \equiv -5 \bmod \mathfrak{p}^{k+1}$.

As before, the order of $\langle -1\rangle \times \langle 1 + 2\sqrt{d}\rangle \times \langle\alpha\rangle$ equals $\phi(\mathfrak{p}^n)$ for any $n \geq 6$. □

5. Primitive Roots in Quadratic Number Rings

As an application of our work, we give a quadratic number ring generalization of primitive roots modulo m in this section.

Definition 6. Fix an algebraic number ring $\mathcal{O}$ and an ideal $\mathfrak{a}$ in $\mathcal{O}$. Then we say that $\alpha \in \mathcal{O}$ is a *primitive root* modulo $\mathfrak{a}$ if and only if $\gcd(\langle\alpha\rangle, \mathfrak{a}) = \langle 1\rangle$ and α has order $\phi(\mathfrak{a})$ in $(\mathcal{O}/\mathfrak{a})^*$.

Plainly, a primitive root modulo $\mathfrak{a}$ exists if and only if $(\mathcal{O}/\mathfrak{a})^*$ is a cyclic group. The following theorem catalogs when primitive roots exist.

Theorem 13. *Suppose that $\mathcal{O}$ is a quadratic number ring.*

(a) There exists a primitive root modulo $\mathfrak{p}^n$ for any prime ideal $\mathfrak{p}$ lying above a split odd rational prime with $n \in \mathbb{N}$, or lying above the split rational prime 2 with $n \in \{1, 2\}$.

(b) There exists a primitive root modulo $\langle p\rangle$ for any inert rational prime p.

(c) There exists a primitive root modulo $\mathfrak{p}^n$ for any prime ideal $\mathfrak{p}$ lying above a ramifying odd rational prime with $n \in \{1, 2\}$, or lying above the ramifying rational prime 2 with $n \in \{1, 2, 3\}$.

(d) If 2 splits in $\mathcal{O}$ with $\mathfrak{p}$ lying above 2, then there exists a primitive root modulo:

- $\mathfrak{p}\langle q\rangle$ *when q is an inert odd rational prime,*
- $\mathfrak{p}\mathfrak{q}^n$ *when $\mathfrak{q}$ lies over a ramifying odd rational prime and $n \in \{1, 2\}$,*
- $\mathfrak{p}\mathfrak{q}^n$ *when $\mathfrak{q}$ lies over a split odd rational prime and $n \in \mathbb{N}$.*

(e) If 2 is inert, then there exists a primitive root modulo:

- $\langle 2\rangle\mathfrak{p}^n$ *when $\mathfrak{p}$ lies over a split odd rational prime $p \neq 3$ and $n \in \mathbb{N}$,*
- $\langle 2\rangle\mathfrak{p}^n$ *when $\mathfrak{p}$ lies over a ramifying odd rational prime $p \neq 3$ and $n \in \{1, 2\}$, and*
- $\langle 6\rangle$ *when 3 is also inert.*

(f) If 2 ramifies in $\mathcal{O}$ with $\mathfrak{p}$ lying above 2, then there exists a primitive root modulo:

- $\mathfrak{p}\mathfrak{q}^n$ *when $\mathfrak{q}$ lies over a split odd rational prime and $n \in \mathbb{N}$,*
- $\mathfrak{p}\langle q\rangle$ *when q is an inert odd rational prime,*
- $\mathfrak{p}\mathfrak{q}^n$ *when $\mathfrak{q}$ lies over a ramifying odd rational prime and $n \in \{1, 2\}$.*

Proof. The assertions (a)-(c) follow directly from our unit group structure theorems from Sections 3 and 4, while the assertions (d)-(f) follow from these same theorems, in conjunction with the fact that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$. □

We give two corollaries of this theorem. The first of these gives the existence of primitive roots modulo an ideal in the Gaussian integers $\mathbb{Z}[i]$ (also given in [3]). Note that since $\mathbb{Z}[i]$ is a PID, any such ideal has the form $\langle\gamma\rangle$ for some $\gamma \in \mathbb{Z}[i]$.

Corollary 1. *A primitive root in $\mathbb{Z}[i]$ modulo $\langle\gamma\rangle$ exists if and only if*

$$\gamma = \pi^n, (1+i)\pi^n, q, (1+i)q, \text{ or } (1+i)^k,$$

where π is a factor of an rational prime $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$ is a rational prime, $n \in \mathbb{N}$, and $k \in \{1, 2\}$.

Proof. This follows immediately from the previous theorem, along with the characterization of primes in $\mathbb{Z}[i]$: A rational prime p is inert in $\mathbb{Z}[i]$ if $p \equiv 3 \bmod 4$, split in $\mathbb{Z}[i]$ if $p \equiv 1 \bmod 4$, and ramifies if $p = 2$. □

The second corollary gives a companion result to the case of the Eisenstein integers $\mathbb{Z}[\omega]$. Again since $\mathbb{Z}[\omega]$ is a PID, any such ideal has the form $\langle\gamma\rangle$ for some $\gamma \in \mathbb{Z}[\omega]$.

Corollary 2. *A primitive root in $\mathbb{Z}[\omega]$ modulo $\langle\gamma\rangle$ exists if and only if*

$$\gamma = \pi^n, 2\pi^n, q, \text{ or } (1-\omega)^k,$$

where π is a factor of a rational prime $p \equiv 1 \bmod 3$, $q \equiv 2 \bmod 3$ is a rational prime, $n \in \mathbb{N}$, and $k \in \{1, 2\}$.

Proof. This follows immediately from the previous theorem, along with the characterization of primes in $\mathbb{Z}[\omega]$: a rational prime p is inert in $\mathbb{Z}[\omega]$ if $p \equiv 2 \bmod 3$, split in $\mathbb{Z}[\omega]$ if $p \equiv 1 \bmod 3$, and ramifies if $p = 3$. □

References

[1] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[2] V. Buçaj, Finding Factors of Factor Rings over Eisenstein Integers, *Int. Math. Forum*, **9(31)** (2014) 1521-1537.

[3] J. Cross, The Euler ϕ Function in the Gaussian Integers, *Amer. Math. Monthly*, **90** (1983) 518-528.

[4] D. Dummit and R. Foote, *Abstract Algebra*, 3rd ed., John Wiley and Sons, New York, 2003.

[5] G. Kohler, *Eta Products and Theta Series Identities*, Springer-Verlag, Berlin, 2011.

[6] D.A. Marcus, *Number Fields*, 2nd ed., Springer-Verlag, Berlin, 1995.

[7] I. Niven, *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1991.

[8] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd ed., AK Peters/CRC Press, Boca Raton, 2001.